Hong Kong Privacy and Data Protection Law 2019 Review

Produced in partnership with ***Dominic Wai of ONC Lawyers***

This Review will highlight cases and incidents of the year 2019 which would be of significant and particular interests to anyone to safeguard himself or herself from incurring criminal and/or civil liabilities by breaching any laws on privacy and data protection.

The year 2019 was an eventful year. Prior to the social movement which happened back in June 2019, there were certain video footages of some celebrities in a private vehicle which the driver shared or uploaded recorded video clips online to social media or selling the clips to a media company without any prior consent from the passengers. The potential liabilities of the driver shall not be overlooked and shall be discussed in the part "**What can you do if a camera in a taxi or hailed car captures your private actions and the video goes viral?**" below. During the social movement, online messages inciting violence against certain groups of people and their families had gone viral. A court injunction was ordered on that but upon subsequent review on the injunction, administrators of online platform are unlikely to be held liable for the information and content published on such platform: "**Injunction against violent online messages: Will online platform administrators be held liable?**". Insofar as the potential liabilities from the use of computer is concerned, the Court of Final Appeal confirms that "obtaining access to computer with a view to dishonest gain" under section 161(1) of the Crime Ordinance should not apply to a person's own device: ***Secretary of Justice v Cheng Ka-Yee and others*** **[2019] HKCFA 9**. However, in ***HKSAR v Chu Tsun Wai*** **[2019] HKCFA 3**, the Court of Final Appeal clarified that the owner's intention of the computer is a key determinant of whether the computer has been misused under section 60(1) of the Crime Ordinance.

The Court of Final Appeal confirms "obtaining access to computer with a view to dishonest gain" should not apply to a person's own device: *Secretary of Justice v Cheng Ka-Yee and others* [2019] HKCFA 9

Facts

Three teachers in a primary school (the "**Primary School**") and a teacher in another primary school (altogether, the "**Four Teachers**") had used mobile smartphones and a school's computer to leak pictures and copies of questions of the admission interview of the Primary School. The Four were charged with violating section 161(1)(c) of the Crimes Ordinance, which prohibits any person who obtains access to a computer with a view to dishonest gain for himself or another. In 2016, the Four Teachers were acquitted by Kowloon City Magistrates' Court where the magistrate

ruled that she was not sure if the three teachers who worked in the Primary School were warned of the confidentiality obligations with respect to the questions of the admission interview and that the prosecution failed to prove the objective limb of the Ghosh test on "honesty" against the Four.

The prosecution then appealed to the Court of First Instance, where it was ruled that using a person's own mobile smartphones, or use of computer which is not authorised, to leak questions did not amount to "obtaining access to computer". The Department of Justice again appealed the decision and the case was eventually determined in the Court of Final Appeal (the "**CFA**").

CFA's Decision

The CFA decided, inter alia, that as a matter of language, one can only "obtain" access to a thing which he or she did not have access to such thing before. Further, the statutory language seems to be redundant as the verb "obtain" is a synonym for "access" when used as a verb. The overlap emphasizes the oddness of applying the charge under section 161(1)(c) of the Crime Ordinance to the use by a person of his or her own computer. Also, considering the legislative history of the relevant section, the interpretive provision "a person obtains access to a computer if (and only if) he causes a computer to perform any function" was deleted. The words "(obtaining access) with or without authority" did not appear in the bill either. The CFA therefore concludes that the charge under section 161(1)(c) of the Crime Ordinance does not apply to the use by a person of his or her own computer which does not involve access to another's computer. The CFA dismissed the prosecution's appeal accordingly.

The charge under section 161(1)(c) of the Crime Ordinance, which prohibits any person who obtains access to a computer with a view to dishonest gain for himself or another, had been used by prosecutors in cases involving stealing of information and breach of privacy by the use of a computer (including a smartphone). Such excessive usage of the charge exceeded the original purpose of the law. The Department of Justice considered that it should cover all computer-related crimes and the objective of the offence was to prevent the improper use of a computer that could lead to a crime. The CFA's ruling in *Secretary of Justice v Cheng Ka-Yee* and others has rectified the situation by narrowing the scope of the charge. As Mr. Justice French NPJ commented in his judgment, it is not the function of the Court to adopt a construction of a statute to advance a desirable public policy. The Court seeks to ascertain the purpose of the statute to inform its construction. It does not identify a purpose which it thinks would be beneficial and then construes the statute to fit it.

DDoS attack – cybercrime for misusing a victim's computer through the victim's website: *HKSAR v Chu Tsun Wai* [2019] HKCFA 3

Facts

On or around October 2014, the Defendant, Mr. Chu Tsun Wai ("**Chu**") took part in a Distributed Denial of Service ("**DDoS**") attack on the website of the Shanghai Commercial Bank ("**SCB**"). Mr Chu was charged with a criminal offence, contrary to section 60(1) of the Crimes Ordinance, namely that he, without lawful excuse, damaged property belonging to another intending to damage such property or being reckless as to whether such property would be damaged.

DDoS is one kind of cyber-attack. The method of a DDoS attack is for a number of co-ordinated computers to send a very large number of requests at more or less the same time to exhaust the server's bandwidth, thereby denying access to persons wishing to transact their ordinary and legitimate business through the website and possibly causing the overloaded system to crash. In the present case, the server of SCB received 504,592 requests within the space of an hour, of which 6,652 came within a space of 16 seconds from Chu's computer (the "**Requests**"). The attack was a failure because the server of SCB had enough surplus capacity to prevent the attack from having any effect upon its other operations.

At the Magistrates' Court, it was found that Chu was the user of the computer launching the DDoS attack to SCB's website and his participation was intentional and that Chu had misused the Bank's computer and convicted Chu. The conviction was upheld upon appeal to the Court of First Instance and Chu appealed to the Court of Final Appeal ("**CFA**").

CFA's Decision

The offence under section 60(1) of the CO is committed when, having obtained access to the computer through the website, one causes it to "function other than as it has been established to function by or on behalf of its owner".

The CFA reasoned that the definition of "misuse of a computer" does not require access as such to have been unauthorised, and it applies to computers which, through their websites, offer open access to the world. The question therefore is how one describes the way in which the computer has relevantly been established to function by its owner.

Chu argued that SCB's computer functioned as it had been established to do because it dealt with the Requests in accordance with what it had been programmed to do. However, the CFA dismissed this argument and was of the view that computers can only do what they have been programmed to do, and that the statute is concerned with what the owner has set it up to do. In other words, the functions for which the computer is established to do are not so much concerned with the way it works (or fails to work) but what it was intended to do. SCB's website and its server were established to provide banking services, not to deal with multitude of requests made for no purpose except to inconvenience SCB and its customers and generate publicity for the attackers. As such, the CFA held that DDoS attack is very appropriately described as a misuse of SCB's computer and that Chu has caused SCB's computer to function other than how SCB has established it to function.

In this case, the CFA provided the legal basis to which cyber-attack on one's website can be regarded as "misuse of a computer" and thus constitutes damage of property under section 60(1) of the CO. In particular, the CFA clarified that the owner's intention of the computer is a key determinant of whether the computer has been misused.

Injunction against violent online messages: Will online platform administrators be held liable?

Background

On 31 October 2019, the High Court of Hong Kong granted an interim injunction, in response to an application filed by the Secretary for Justice of Hong Kong, to ban anyone from posting or spreading messages online inciting the use or threat of violence that would cause "bodily injury to any person unlawfully" as well as "damage to any property unlawfully" (the "**Injunction**"). The Injunction was challenged by the Internet Society of Hong Kong Limited ("**ISOC**") (HCA 2007 / 2019), seeking the discharge of the Injunction or variation of its terms.

ISOC submitted that knowledge is a required element for both the criminal offence of incitement and for the tort of public nuisance. If the specific requirements of knowledge of both the quality of the material and that the publication is intended to cause bodily injury or damage are not included, the Injunction would catch unwitting and unintended bona fide posters and those who post for a legitimate purpose, e.g. the online platform operators. ISOC suggested that the wording of the Injunction shall be crafted in simple ways to include the requisite knowledge elements.

Decision

Hon Coleman J of the Court of First Instance of the High Court ruled that the Injunction shall not be discharged. Nonetheless, the terms of Injunction were slightly amended to protect the innocent internet providers and online platform administrators by adopting wording linking publication to its purpose.

When considering the four-stage proportionality test in *Hysan Development Co Ltd v Town Planning Board* (2016) 19 HKCFAR 372, among the others, the Court is of the view that that there was no problem in requiring publishers of material to exercise some self-censorship which the Court suggested it is not necessarily a bad thing, and the Court did not think the Injunction imposed an unacceptably harsh burden on any person to be asked to exercise their rights and freedoms with a degree of responsibility. Nonetheless, the court decided to amend the Injunction slightly to include wordings including "for the purpose of" and "wilfully" in order to protect online platform administrators from criminal liabilities who are usually without knowledge of the fact and contents of any publication on their platform.

Online platform administrators shall be relieved that with such slight amendment to the Injunction order, even if they allow posts to be made on their platforms, without knowing the fact of the publication or the contents of the publication, they cannot be said to be in breach of the Injunction. The Court has made clear that the Injunction would only ban online materials published "for the purpose of" promoting, encouraging or inciting the use or threat of violence and could only restrain people who "wilfully" assist others to commit such acts. This will be particularly crucial for online platform administrators involving dissemination of materials from the sending of private messages on the platforms or concern arising from an inability to know how any particular receiver of the message will understand the content of the message.

What can you do if a camera in a taxi or hailed car captures your private actions and the video goes viral?

Introduction

Video cameras have been installed inside some taxi and hailed car compartments in Hong Kong for security and safety purposes. They would record the video images of the passengers. Some unscrupulous drivers might share or upload the recorded video clip online to social media or sell the clip to a media company without any prior consent from the passengers. A recent example for this was the leakage of video footage involving certain celebrities last year.

Regarding the potential serious intrusion into the passengers' private lives as a result of the leakage of the unauthorised video recording, the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") has procedural safeguards and imposed various obligations on data users through the six data protection principles ("**DPP**") as stipulated in Schedule 1 to PDPO. A breach of DPP amounts to a contravention of PDPO. Data users, including but not limited to taxi or hailed car drivers, may face civil and criminal proceedings as a result of the unauthorized disclosure of the recording.

Liabilities of taxi / hired car drivers

If the video clips recorded inside the taxi or other vehicles have been widely distributed, only the data subjects, namely the persons captured in the tapes can lodge a complaint to the Privacy Commissioner for Personal Data (the "**Commissioner**") under section 37 of PDPO regarding any contravention of PDPO. Once the Commissioner receives a complaint, he may investigate and thereafter publish case notes of his investigation. If the Commissioner finds that the data user has breached PDPO, enforcement notice will be served on the data user requesting him to rectify the contravention or refrain from acting in contravention of PDPO. According to section 50A of PDPO, non-compliance of the enforcement notice will attract a maximum sentence of 2 years imprisonment and a fine of HK$50,000. The Commissioner may also refer such noncompliance or any criminal offence under PDPO to the Police for prosecution.

Further or in the alternative to lodging a complaint, if a contravention of PDPO causes the data subjects loss or injured feelings, civil proceedings in the District Court could be commenced for compensation under section 66 of the PDPO.

There are certain grounds that taxi or other drivers and other data users may be sued, and certain precautionary measures are advised to be taken by them. For instance, according to DPP 1 of the PDPO, collection of personal data shall be lawful, fair and not excessive. It also requires data users to take all reasonably practicable steps to inform the data subject of the following when collecting the subject's personal data. As such, taxi or other drivers and other data users shall notify the passengers of the existence of the video camera inside the taxi or car compartment by, for example, affixing notices on the inner parts or the exterior of the taxi or car, so that the passengers can choose whether to get on the taxi or hailed car. Failure to do so shall be considered as a breach of DPP 1 of PDPO. Additionally, it is a criminal offence for a person who obtains personal data from a data user without the data user's consent and discloses that personal data with the intent to obtaining a gain or cause loss to the data subject, or in circumstances where the disclosure causes psychological harm to the data subject, according to section 64 of PDPO. Such offence carries a maximum punishment of HK$1 million fine and five-year imprisonment. The Commissioner shall bear the responsibility to prosecute any person who contravenes section 64 of PDPO.

Taxi and other hailed / hired car drivers should be aware of the legal implications of using and circulating the video clips recorded in the taxi or hailed car for purposes not originally intended or unlawful. It is also prudent for them to post a sign of, for instance, "Recording in progress", or "The taxi is equipped with camera security" in their vehicle. Should the video clips be published, the passengers being recorded may lodge a complaint and commence civil proceedings against the recorders and the publishers with a view to protecting their privacy.

Author

Dominic Wai

Partner, ONC Lawyers

Before joining the legal profession, Dominic has worked in the banking sector and as well as in the Independent Commission Against Corruption (ICAC).

Dominic's practice focuses on advising clients on matters relating to anti-corruption, white-collar crime, law enforcement, regulatory and compliance matters in Hong Kong, including advice on anti-money laundering. He also handles cases involving corporate litigation, shareholders' disputes and insolvency matters, defamation cases, domestic and international arbitration cases, cybersecurity, data security and privacy law issues, competition law matters, e-Discovery and forensic investigation issues as well as property litigation.

Dominic is currently a board member of a charity that provides a home service for sick children and their families. He is supportive and actively participating in the activities of the charity.
